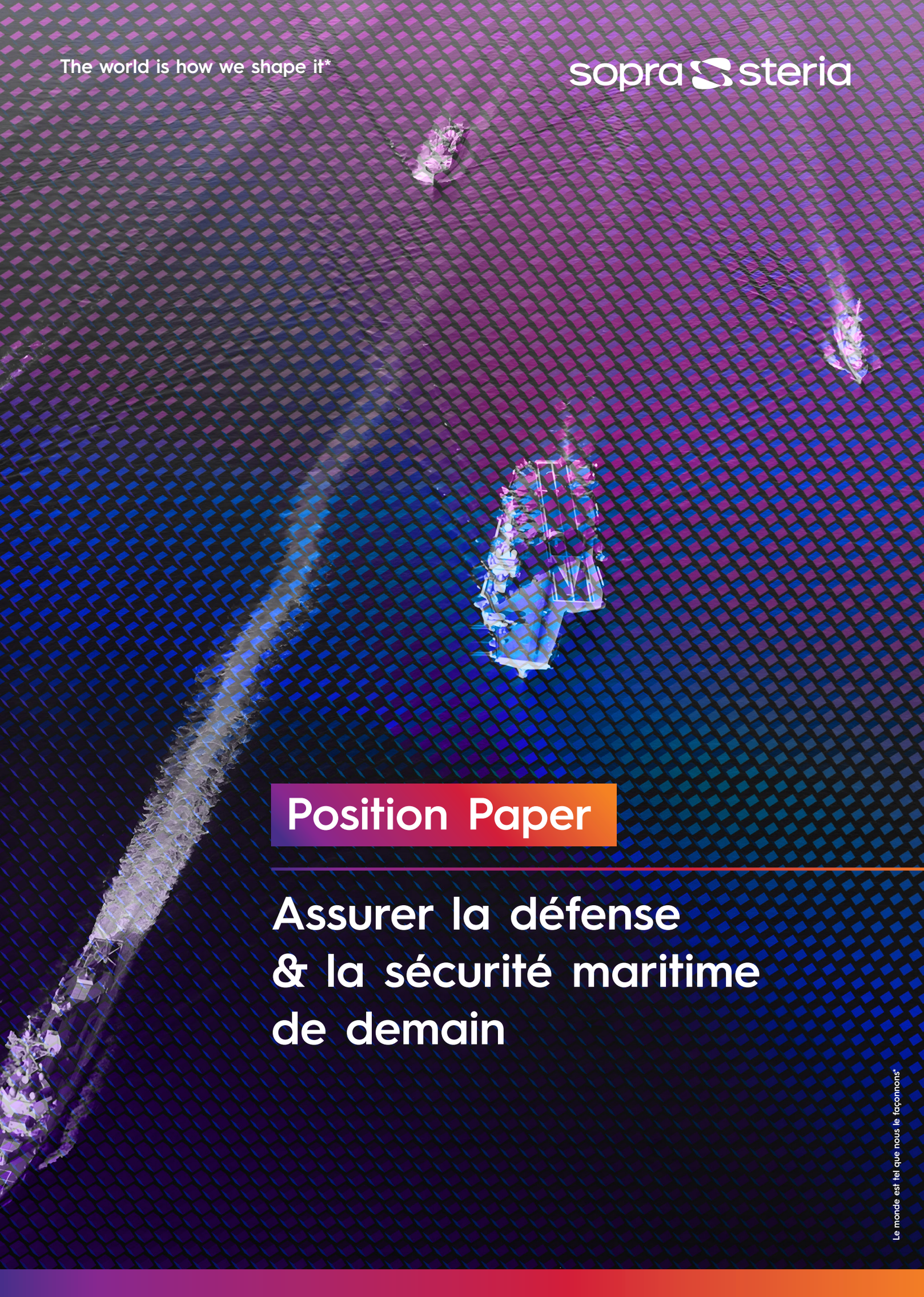
The world is how we shape it*

sopra steria



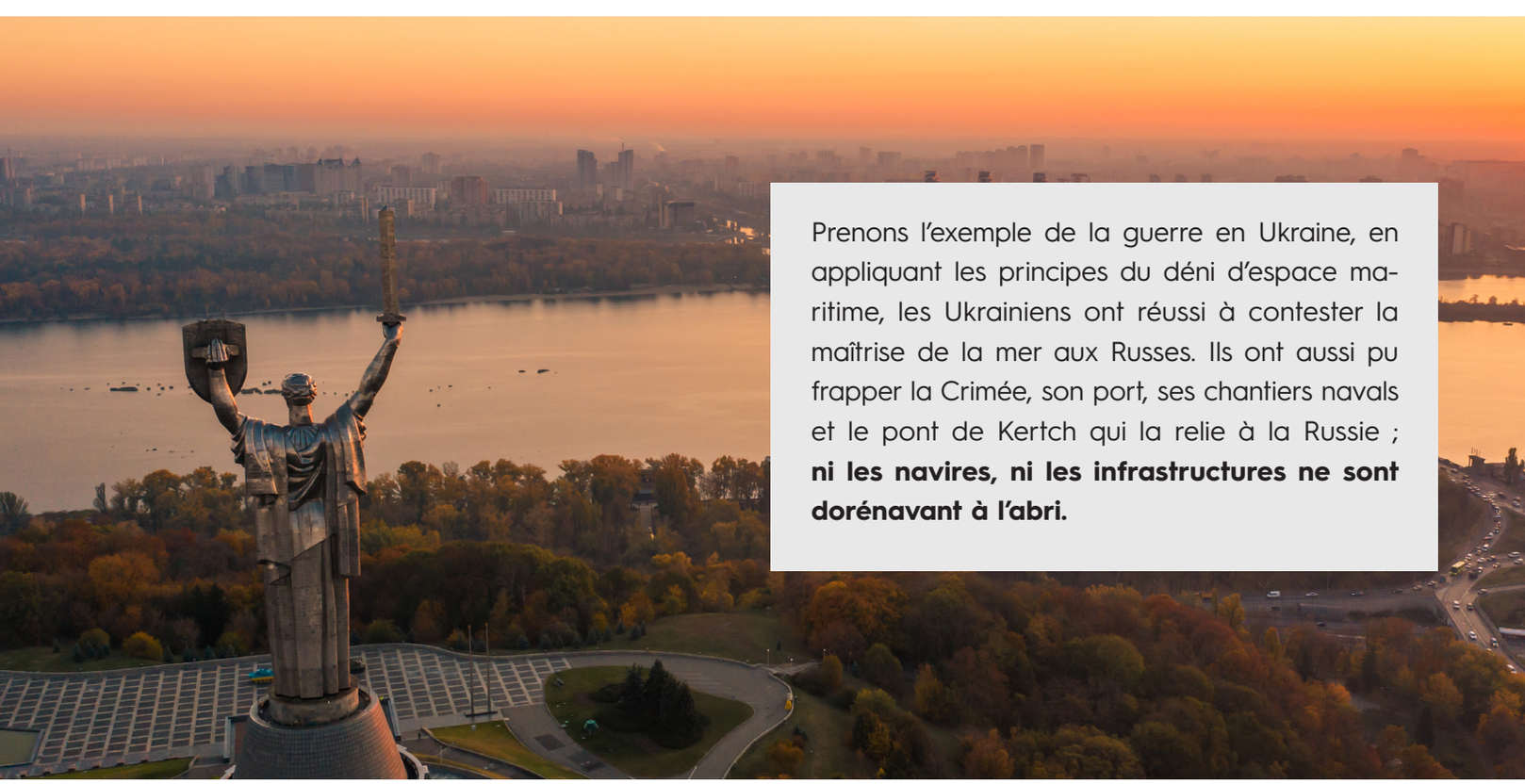
Position Paper

# Assurer la défense & la sécurité maritime de demain

Le monde est tel que nous le façonnons*

Le monde tel que nous l'avons connu est en train de changer. L'ordre international post-Seconde Guerre mondiale est de plus en plus contesté. Les conflits larvés ou ouverts peuvent s'égrener dans une longue litanie : guerre entre la Russie et l'Ukraine, conflit entre Israël et le Hamas mais aussi le Hezbollah et l'Iran, opération terrestre menée par Tsahal au sud-Liban, guerre au Soudan, tensions en mer de Chine, au Cachemire et même en Arctique, etc. Aucun continent ni océan n'est épargné. Les ambitions s'aiguisent, les nations se réarment et « partout, les empires se réveillent.[1] »

La France dispose de la deuxième plus grande zone économique exclusive (ZEE) au monde, derrière les États-Unis. C'est dans un contexte international en très forte tension qu'il faut appréhender les enjeux maritimes, des grands fonds au spatial. Au regard de la fragilité du contexte international et de la rivalité pour le contrôle des richesses et des voies maritimes, la protection du domaine maritime est un objectif stratégique pour la défense de la France et plus largement de l'Europe.

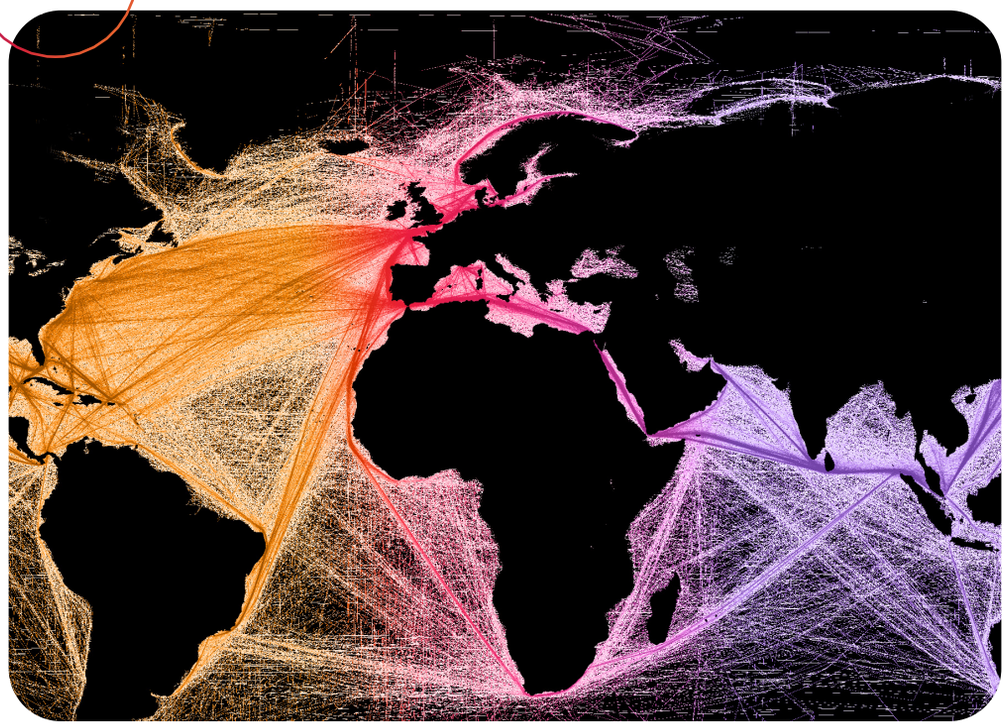


Prenons l'exemple de la guerre en Ukraine, en appliquant les principes du déni d'espace maritime, les Ukrainiens ont réussi à contester la maîtrise de la mer aux Russes. Ils ont aussi pu frapper la Crimée, son port, ses chantiers navals et le pont de Kertch qui la relie à la Russie ; **ni les navires, ni les infrastructures ne sont dorénavant à l'abri.**

**1** Alain Bauer, « La doctrine militaire russe et les leçons à en tirer », Revue Défense nationale, Tribune no 1386, 6 mai 2022, p. 10.

La sécurisation des routes commerciales maritimes, des personnes et des biens est également l'un des grands enjeux du XXIe siècle. On le voit clairement en mer Rouge et dans le détroit d'Ormuz, par exemple, avec les interventions de la Marine nationale et de ses alliés, pour lutter contre les attaques houthis qui cherchent à perturber le trafic maritime. Notons que le Yémen utilise aussi ses munitions téléopérées contre Israël engagé dans un combat d'usure contre le Hamas.

Le groupe Sopra Steria, dont sa filiale CS Group, réaffirme son engagement et sa contribution à la défense et à la sécurité maritime. Acteur souverain, partenaire de confiance des systèmes et services critiques du secteur Défense, Sopra Steria anticipe le monde maritime de demain et le construit avec les acteurs défense et sécurité, conscient des risques qui pèsent sur les mers, les océans, les grands fonds marins, les côtes et les ports du globe.



# Stratégie pour répondre au contexte

## Les grands axes et enjeux



# 01.



## Renforcer les fonctions et processus opérationnels

Garantir la capacité d'effectuer les missions de la Marine - Dissuader, Protéger ( y compris la protection des populations et des flux maritimes) , Connaitre (renseignement) et anticiper, et Intervenir (dont l'assistance en mer) nécessitent une organisation capacitaire robuste et agile, une colonne vertébrale RH solide et adaptable et une boucle décisionnelle des opérations capable de répondre aux nombreux défis liés à la variété des menaces dans l'ensemble des milieux et des champs (MDO).

### 1 Revoir à la hausse le plan d'armement des navires

L'engagement accru de la Marine, et la pression résultante sur la disponibilité de parcs d'équipements vieillissants et sur l'approvisionnement en munitions, est au cœur des préoccupations des états-majors. Réarmer qualitativement les navires, en optimisant le MCO, en mettant en réseau des équipements de défense existants, ou en adoptant des systèmes de rupture (AED, effecteurs EM, etc.) est essentiel à la supériorité stratégique.[2]

### 2 Rénover, renouveler les infrastructures portuaires

Les opérations de rénovation destinées à la mise à niveau et au renouvellement des capacités de la Marine sont un engagement technico-financier essentiel à la bonne conduite des programmes d'équipement et d'armement en phase de création et de maintenance sur le long terme.

**2** Centre d'Etudes Stratégiques de la Marine, « Etudes navales – La Marine nationale au service des Français », mars 2022

## 3 Renforcer la capacité immédiate à combattre

### a Développer l'entraînement en ambiance haute intensité

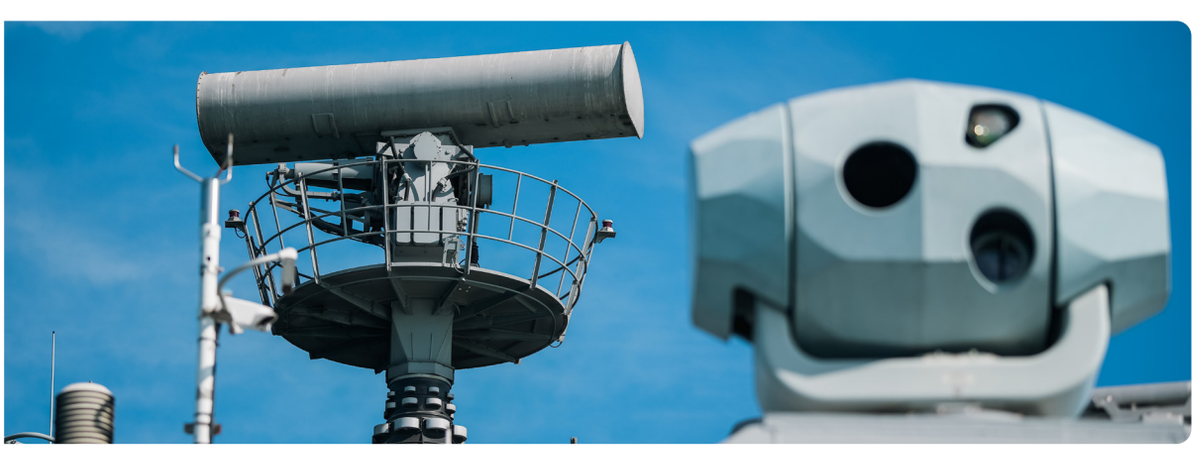
Le durcissement des opérations en mer oblige à retrouver un niveau d'entraînement permettant de faire face à la haute intensité. **Des exercices majeurs complexes**, au plus proche des conditions de l'engagement symétrique multi-domaines, doivent permettre l'aguerrissement des équipages, tout en permettant aux officiers et aux états-majors de rénover les concepts tactiques et opérationnels au cœur de ces déploiements.

### b Capacité à combattre en mode dégradé

L'évolution des menaces requiert la capacité d'y répondre « **en mode dégradé** ». L'approfondissement de la veille coopérative navale (VCN), visant à établir une situation tactique via l'échange d'information entre plusieurs unités, répond à cet objectif. Le combat collaboratif, et la capacité de combattre « à l'aveugle » grâce aux données fournies par des unités alliées, sont essentiels à la résilience de la Marine.[3]

### c Connectivité Mer – Terre - Espace, horizontal et vertical

L'optimisation du Command & Control dans un contexte d'extension du partage de la donnée interalliés/interarmées, inscrivent **l'espace et le cyber** en continuité avec les opérations navales. Parallèlement, **les champs électromagnétique et informationnel** sont des théâtres d'opérations à part entière nécessitant d'être articulées aux opérations navales. L'accroissement de la nature multi-milieux multi-champ (M2MC) des conflits doit engager un processus de maîtrise de l'ensemble du spectre de la conflictualité.



**3** Opex360, « la FDA Forbin tire un Aster-15 en «mode dégradé» tandis que la FREMM Bretagne s'initie au combat collaboratif », 1 juin 2023




# L'anticipation des ruptures technologiques et l'interopérabilité

## 1 Engagement dans la préparation au combat data-centré

La stratégie de supériorité informationnelle pour la guerre navale doit aboutir à une marine capable de capter, fusionner et valoriser la donnée pour maîtriser une situation tactique et prévenir l'effet de surprise. Un engagement de la Marine dans des **programmes de plateformes data-centrées et prêtes au combat M2MC collaboratif** est un gage de résilience opérationnelle.

## 2 Robotisation et automatisation des capacités

Face à l'accélération de la mutation numérique, une démarche volontariste est requise pour **s'approprier les nouvelles capacités liées à la dronisation et l'automatisation** des armées, et développer des capacités de lutte anti-drones (LAD) pour protéger les matériels – y compris les drones eux-mêmes. La robotisation des forces de compétiteurs stratégiques doit conduire à une réflexion sur l'usage de ces outils à chaque échelon de son activité : dans les bâtiments, les infrastructures au sol, la chaîne logistique et le MCO.

## 3 Développement de la culture de prospective

Garantir la supériorité à la mer de la Marine requiert de **stimuler la réflexion stratégique** de ses décideurs, au moyen d'outils aussi variés que les ateliers de prospective, les simulations de crises et autres *wargames*. En effet, anticiper les évolutions et les ruptures géopolitiques et techniques est un défi à la complexité croissante mais dont la pratique est un gage de survie face au risque de déclassement.

# Sopra Steria - CS Group
## les fondements de notre vision

Innovations, technologies de rupture et prospective



# 02.

**Pour répondre à l'ensemble de ces enjeux, le groupe affirme ses convictions & déploie des solutions innovantes et souveraines au plus près des besoins des forces.**

### L'innovation : intégrer plus vite les innovations prometteuses qui deviendront les capacités déterminantes de demain

Dans un monde de plus en plus complexe et tendu, innover c'est conserver une supériorité technologique sur les adversaires de la France, de l'Union européenne et de l'OTAN, garantir notre sécurité, et garder une longueur d'avance sur les compétiteurs.

Le cycle des technologies est en pleine accélération, il faut donc réduire le temps de leur intégration dans l'Armement, notamment en adaptant des innovations civiles. Ces technologies doivent permettre une meilleure détection de la menace, des armes plus efficaces, une organisation interalliée plus efficiente et le développement d'outils d'aide à la décision permettant une supériorité informationnelle afin d'obtenir une amélioration significative de l'efficacité opérationnelle.

L'environnement militaire de plus en plus complexe nécessite une vue d'ensemble et une démarche d'innovation technologique forte pour une adaptation constante aux contraintes évolutives de ce secteur. Industriel du numérique de Défense,  le groupe Sopra Steria imagine avec ses clients des solutions sur mesure mettant le numérique au service de l'humain.

L'innovation technologique dans le secteur de la défense et de la sécurité est essentielle pour répondre aux défis contemporains. Le groupe s'engage à développer des solutions souveraines qui contribuent à renforcer l'autonomie stratégique de l'Europe. En collaboration avec des partenaires dans le cadre de projets européens de recherche et d'innovation, nous concevons des systèmes avancés cyber sécurisés intégrant des technologies d'intelligence artificielle et de traitement des données en temps réel. De plus, notre approche est résolument tournée vers l'interopérabilité entre les différents acteurs, contribuant ainsi à améliorer l'efficience des opérations.

### Data & IA : optimiser les capacités actuelles en opérations et valoriser la supériorité informationnelle

Dans un environnement multi-domaines complexe et dual, l'IA intégrée dans des systèmes de Commandement, de Contrôle et de conduite d'opérations doit permettre de déceler l'information utile et validée et réduire la boucle OODA (Observation, Orientation, Décision, Action) pour éviter la saturation cognitive dès 2040. Cela exige des progrès dans les technologies et une adaptation de l'IA. Notre objectif à terme est d'obtenir une IA décisionnelle pouvant soutenir le Command and Control (C2) en tout temps et en toute confiance.

Ce dernier point est crucial car l'IA devant guider l'action militaire, elle n'a de valeur que si elle est fiable. Sopra Steria croit que l'IA de confiance – protégée contre les cyberattaques et respectant des règles éthiques (équité, vie privée, non-discrimination, etc.) – est la seule à même de valider, de certifier et d'expliquer ses résultats. C'est cette conviction qui nous a amené à intégrer le collectif Confiance.ai qui conçoit et industrialise des systèmes à base d'IA de confiance aux côtés de près de 50 partenaires.

La nature connectée de la guerre, évidente étant donné les moyens dont disposent les armées (missiles, satellites, drones, etc.), va s'intensifier dans les années à venir. Garantir une expertise dans les domaines de la gestion de la data et des algorithmes analytiques, permet d'assurer une adaptabilité face aux menaces en mers toujours plus prégnantes.



**Tenir dans la durée**

Quel que soit le champ de bataille, le temps est la clé. Les belligérants cherchent à durer et comme le souligne l'amiral Vaujour, les conflits d'aujourd'hui et de demain posent la question de l'usure et de la décision . Depuis de nombreuses années, nous avons misé sur les armes de décision. Aujourd'hui et plus encore demain, nous avons besoin d'arme d'usure, comme le drone, qui permettent de saturer les défenses adverses. L'objectif est bien de tenir dans la durée.

Usure et décision vont de pair, un équilibre est à trouver. Les essaims de drones sous-marins expérimentés lors de l'exercice Orion entrent dans ce cadre. User l'adversaire pour durer ne peut se résumer à une profession de foi, par ailleurs nécessaire. Cet objectif indispensable pour le succès des armées doit bien sûr s'accompagner d'un appel à l'action déterminé.

### Le quantique : se préparer à une révolution des moyens de calcul et de cryptage des données

« *Les technologies quantiques sont à un moment charnière* », souligne le physicien Julien Bobroff. Ces technologies ne se résument pas à la cyberdéfense et aux réseaux de communication ou à la cryptographie. Elles couvrent un bien plus large spectre de domaines militaires, à travers ses trois grands champs d'applications : la cryptographie, les capteurs et l'ordinateur (optimisation et simulation). Dans ces trois segments, les applications défense sont multiples : spatial militaire, télécommunication, localisation ou furtivité des sous-marins, détection d'armes NRBC, santé, nouveaux matériaux, etc.

Conscient de cet enjeu majeur, Sopra Steria a depuis plusieurs années mis en place une veille technologique et travaille avec des partenaires intégrés au fond Quantonation qui explore des domaines tels que la conception moléculaire, le calcul haute performance, la cybersécurité ou la détection ultraprécise. Le quantique n'offrira pas seulement des améliorations et de nouvelles capacités, mais imposera également de faire évoluer les doctrines et les concepts d'emploi du niveau tactique au niveau stratégique.

**5** Commission des affaires étrangères, de la défense et des forces armées : compte rendu de la semaine du 13 novembre 2023

### La prospective : initier une démarche de réflexion et de préparation aux enjeux à venir

Comme l'assenait Guilio Douhet : « *La victoire sourit à ceux qui anticipent l'évolution du caractère de la guerre, pas à ceux qui s'y adaptent une fois que le changement est intervenu.* ». A l'aube d'une accélération majeure des cycles d'innovation civilo-militaires, il convient de maintenir cette démarche d'anticipation afin d'entrevoir les usages des technologies en cours de maturation pour les 20 années à venir.

Qu'il s'agisse d'innovations proches de l'industrialisation – Edge computing, jumeaux numériques – ou de systèmes en développement – radars quantiques, armes à énergie dirigée – réfléchir dès maintenant à leur intégration dans le modèle économique, logistique et opérationnel des armées de la prochaine décennie est indispensable à une préparation correctement exécutée. C'est ce besoin qui conduit Sopra Steria à accompagner ses partenaires et clients dans une démarche de réflexion prospective pour déterminer la meilleure manière de répondre à des besoins à long-terme.



Commandement & Contrôle, cyberdéfense, renseignement, lutte informationnelle, sûreté, maintenance et logistique : dans tous ces registres critiques, le groupe innove et s'appuie sur les IA génératives et extractives, mais aussi sur les progrès quantiques et les technologies cloud, pour concevoir et déployer des solutions ultra-sécurisées, sur mesure et haute performance pour ses clients-partenaires.

# Sopra Steria - CS Group

## Des solutions opérationnelles au plus près des besoins de la marine



# 03.

## Nos solutions de Command & Control (C2), de liaison de données tactiques et d'entrainement

L'interopérabilité, la fusion multi-capteurs, la simulation, la sécurisation des données et des infrastructures, sont autant de domaines maîtrisés par le groupe et déployés au travers de solutions souveraines.

CS GROUP affiche une expertise reconnue en matière de liaisons de données tactiques, notamment L16 et L22. Son savoir-faire en gestion de réseau garantit une surveillance en temps réel et une maintenance des réseaux tactiques, tandis que ses solutions C2 favorisent, à l'image de **STARLINX** (Système C2 tactique), une vision partagée de la situation et des capacités avancées de débriefing et d'évaluation des engagements.

**TACTX** permet quant à lui de simuler des échanges multi-Link et assure des tests en environnements virtuels, afin de vérifier la conformité de différentes plateformes aux standards en vigueur.

Par ailleurs, grâce à ses compétences en simulation, CS GROUP offre des outils performants pour la création de scénarios opérationnels immersifs et de modèles intelligents, permettant une formation réaliste au combat de haute intensité.




Les outils de Virtual Simulation, tels que **FIGHTER X** et **UAV X**, offrent aux opérateurs une formation immersive en temps réel, permettant de préparer le personnel entrainé dans des environnements tactiques dynamiques. Ces outils intègrent des liaisons de données tactiques simulées, garantissant une formation complète tout en facilitant l'évaluation des performances à l'échelle d'une opération.

**Direct CGF** génère quant à lui des forces et des unités simulées pour recréer des scénarios militaires réalistes dans des environnements virtuels. Ces entités autonomes interagissent avec les forces humaines ou simulées, en suivant des comportements programmés qui reproduisent les tactiques, les mouvements et les stratégies à l'œuvre sur un champ de bataille. **Direct CGF** permet ainsi de tester des plans d'opération, d'entraîner les opérateurs et d'évaluer les systèmes dans des situations variées sans avoir besoin de mobiliser des forces réelles.

Enfin, la combinaison de ces solutions permet de créer et animer des scénarios complexes d'entraînement les plus réalistes possibles en intégrant la liaison 16 et utilisant celle-ci pour transporter des données simulées. Déjà utilisée par les trois armées, notamment par la Marine nationale, le programme **JEANNETTE** consiste à densifier les missions en combinant le réel (L comme Live), le virtuel (V) par le biais de simulateurs pilotés et le constructif (C) par l'injection d'éléments générés par **Direct CGF.**




## Nos solutions de Data Centric Security & de supervision de la sécurité

Sopra Steria croit en l'interopérabilité et l'interconnexion entre les armées ; nous pensons que la **DCS** – Data Centric Security – contribuera à terme à réduire les redondances de réseaux multiples pour ne constituer qu'un seul et unique réseau qui facilitera les échanges, le partage et la consommation de données. Nous participons aux études et réflexions concernant la mise en œuvre de la **DCS** qui permettra de fusionner tous les réseaux et ainsi de faciliter l'interconnexion entre les pays et leurs armées.

Forte de son expérience avec le ministère des Armées pour la supervision de systèmes complexes avec des exigences de sécurité très élevées et des contraintes matérielles importantes, Sopra Steria a construit une suite de supervision de sécurité innovante, adaptative et souveraine. **MACTAN** apporte aux secteurs régaliens comme les industries de la défense, du transport et de l'énergie une solution clé en main et sur-mesure alliant pertinence et performance de la détection.

Les bénéfices de **MACTAN** :

- Une protection à grande échelle pour faire face aux enjeux du Big Data.
- La prise en compte des contraintes réseaux et les architectures distribuées pour une adaptation aux SI décentralisés ou centralisés, et une intégration avec les autres outils de la sécurité des SI comme les NDR et les EDR.
- L'application des plus hautes règles de confidentialité et de sécurité conformément aux exigences de nos clients étatiques.
- Une empreinte matérielle minimale pour réduire les coûts économiques et écologiques en lien avec les engagements de Sopra Steria pour un numérique plus responsable.

## Nos solutions de protection portuaire

Dans un tout autre domaine, CS GROUP a conçu plusieurs solutions innovantes pour renforcer la sécurité des infrastructures portuaires militaires. Parmi elles, le **Maritime Warning and Protection System** (MWPS) nous a permis d'améliorer notre R&D et nos expériences et de créer **SEMAPORT**, une solution intégrée dédiée à la surveillance des bases navales. Ce système combine la veille caméras, le suivi des objets, la récupération de données AIS et l'identification optronique en continu, de jour comme de nuit. Grâce à une gestion multi-capteurs, **SEMAPORT** offre une cartographie précise des zones surveillées et assure une gestion optimisée des pistes, en permettant une classification rigoureuse des contacts détectés.

CS GROUP déploie également sa solution **CRIMSON**, socle C2 multi-domaines, pour le projet **SIPS** (système intégré de protection des bases de défense). Ce système est actuellement en phase de déploiement dans les bases militaires et équipera huit sites de la Marine nationale.

**CRIMSON**, par ailleurs déjà largement employé par la sécurité civile, joue un rôle central dans la coordination des opérations de sécurité et la gestion des menaces, en s'intégrant parfaitement aux autres systèmes développés par CS GROUP. Il peut notamment être connecté aux systèmes anti-drones conçus par CS GROUP (voir ci-après), tout comme à des générateurs de simulation tel **Direct CGF**, idéal pour l'entrainement des forces. C'est sur **CRIMSON** que se fonde l'offre de Command & Control Multi-domaines portée par CS GROUP.

CS GROUP propose également le système **TIAMAT** (Threat Identification Assistance for Maritime Awareness Technologies). Ce dernier repose sur des technologies avancées d'intelligence artificielle pour détecter, reconnaître, suivre et classifier les bateaux. **TIAMAT** permet ainsi une analyse fine et en temps réel des objets maritimes grâce à ses classifieurs IA, renforçant considérablement la capacité de vigilance en milieu maritime. Des expériences sont en cours avec notamment **TIAMAT** Nuit pour un système 24/24 et **TIAMAT** embarqué sur un navire militaire, couplé à la lutte anti-drones et au C2 de CS GROUP.



Ainsi, CS GROUP contribue de manière significative à la protection et à la sécurisation des infrastructures portuaires et navales, en combinant technologie optronique, radar, intelligence artificielle, et fonctions C2 centralisées.



## Nos solutions de lutte anti-drones

CS GROUP est depuis 2015 un pionnier et un leader reconnu dans le domaine de la lutte anti-drone (C-UAS). CS GROUP a remporté, puis déployé avec succès d'importants contrats pour des acteurs étatiques clés, ainsi que pour des acteurs européens majeurs de la sécurité, parmi lesquels le ministère des Armées français, la préfecture de Police de Paris ou l'Union européenne. Autour de **BOREADES**, cœur C2 tout spécialement conçu pour la LAD, CS GROUP intègre des solutions adaptées au besoin de ses clients.

Dans ce registre, après avoir développé le système **RADIANT** en 2016 pour la préfecture de Police de Paris, puis déployé sur plusieurs emprises militaires le système **MILAD** (Moyens mobiles de lutte anti-drones), CS GROUP a conçu, en coopération avec THALES, le système **PARADE** (Protection déployable modulaire anti-drones).

À noter que CS GROUP a également conçu le système **ARLAD**, installé sur des véhicules militaires de l'armée de Terre, permettant ainsi une grande flexibilité de déploiement sur les théâtres d'opération. Il peut être utilisé dans des zones de conflit ou sensibles, en protection de convois, offrant une solution mobile face à la menace drones.

Conscient des besoins d'interopérabilité des systèmes, CS est également très engagé dans l'implémentation des standards (SAPIENT) pour favoriser l'intégration des différents capteurs et effecteurs à son C2. Son expertise dans le domaine de la liaison de données tactiques lui permet également d'intégrer son système de lutte anti-drone au dispositif de défense aérienne.

**Références opérationnelles**

- PPP (Police Paris) : **RADIANT**. Protection d'évènements majeurs, dont tous les défilés du 14 Juillet, Euro 2016, Ryder Cup, Coupe du monde 2019, coupe des Six nations 2023, Coupe du monde de Rugby 2023, Jeux Olympiques de Paris 2024, etc.
- DGA : **MILAD**, 18 systèmes opérationnels pour la protection de sites en France et en OPEX pour le ministère des Armées, plusieurs systèmes lourds et légers, déployés durant les JO et les JO 2024
- DGA : **PARADE** (en partenariat avec THALES) : 6 systèmes, déploiement lors des JO et des JOP 2024
- Armée de Terre (STAT) : **ARLAD**, système mobile intégré sur véhicule de l'avant blindé (VAB), déploiements en OPEX, 18 systèmes livrés
- Protection anti-intrusion de sites industriels critiques
- Ethiopian Airlines : déploiement du système opérationnel C-UAS à l'aéroport Bole Addis Abeba, en 2023

JOP 2024 : CS GROUP a déployé avec succès 14 dispositifs de détection et de neutralisation de drones parmi lesquels plusieurs systèmes **PARADE** et **MILAD**, déployés et opérés par l'Armée de l'Air et de l'Espace, l'Armée de Terre et la Marine nationale, ainsi que des systèmes **RADIANT** conçus pour la Préfecture de Police de Paris. CS GROUP a également fourni plusieurs systèmes légers permettant de compléter la couverture dans les environnements complexes que représentent les zones urbaines denses.

Ces nombreuses références opérationnelles garantissent un niveau de performance optimal disponible sur le marché pour les solutions C-UAS intégrées par CS GROUP autour du **C2 BOREADES**. Parallèlement, CS GROUP est engagé dans un processus d'amélioration continue et d'innovation pour garantir que sa solution reste à l'état de l'art, face aux menaces en constante évolution, avec une performance optimisée quel que soit le milieu.

## Nos solutions embarquées

Le contexte opérationnel des marines est en perpétuelle évolution et les marins doivent assurer leurs missions dans un climat de cyber agression et de guerre électronique, comportant de forts risques de brouillage et leurrage des solutions de radio navigation (GNSS). L'exactitude des informations de navigation, leur distribution en temps réel et la résistance aux menaces externes sont primordiales pour assurer l'ensemble des missions d'un bâtiment.

Pour faire face à un tel contexte, CS GROUP a développé le MILGPS Receiver, un récepteur GPS certifié anti-spoofing, conçu pour être utilisé à la fois sur des navires de surface et des sous-marins. Ce récepteur offre une protection robuste contre les tentatives de manipulation des signaux GPS, assurant ainsi une navigation fiable et sécurisée.

En complément, l'antenne MIL-CRPA-4 représente la solution ultime de CS GROUP pour contrer le brouillage des signaux GPS. Grâce à cette technologie complémentaire, les navires bénéficient d'une protection avancée contre le brouillage, ce qui est crucial pour la précision et la continuité des systèmes de navigation dans des environnements perturbés.

CS GROUP a également développé le NDDS (Navigation Data Distribution System). Couplé à la centrale inertielle TopAxyz conçue par THALES, ce calculateur met en œuvre les dernières avancées technologiques en matière de cybersécurité garantissant le meilleur niveau de résilience aux agressions. Son architecture offre 3 avantages clés : une navigation plus sûre, une réduction des coûts et des risques d'intégration, la facilité d'utilisation et de maintenance simplifiée du système.



Dans un autre registre, CS GROUP a développé le GMU (Gun Monitor Unit) pour le calcul de la trajectoire balistique et le pilotage du canon au sein de la chaîne d'artillerie, en interface avec l'optronique et les radars du bâtiment de surface, avec le Système de Combat ou en autonomie.

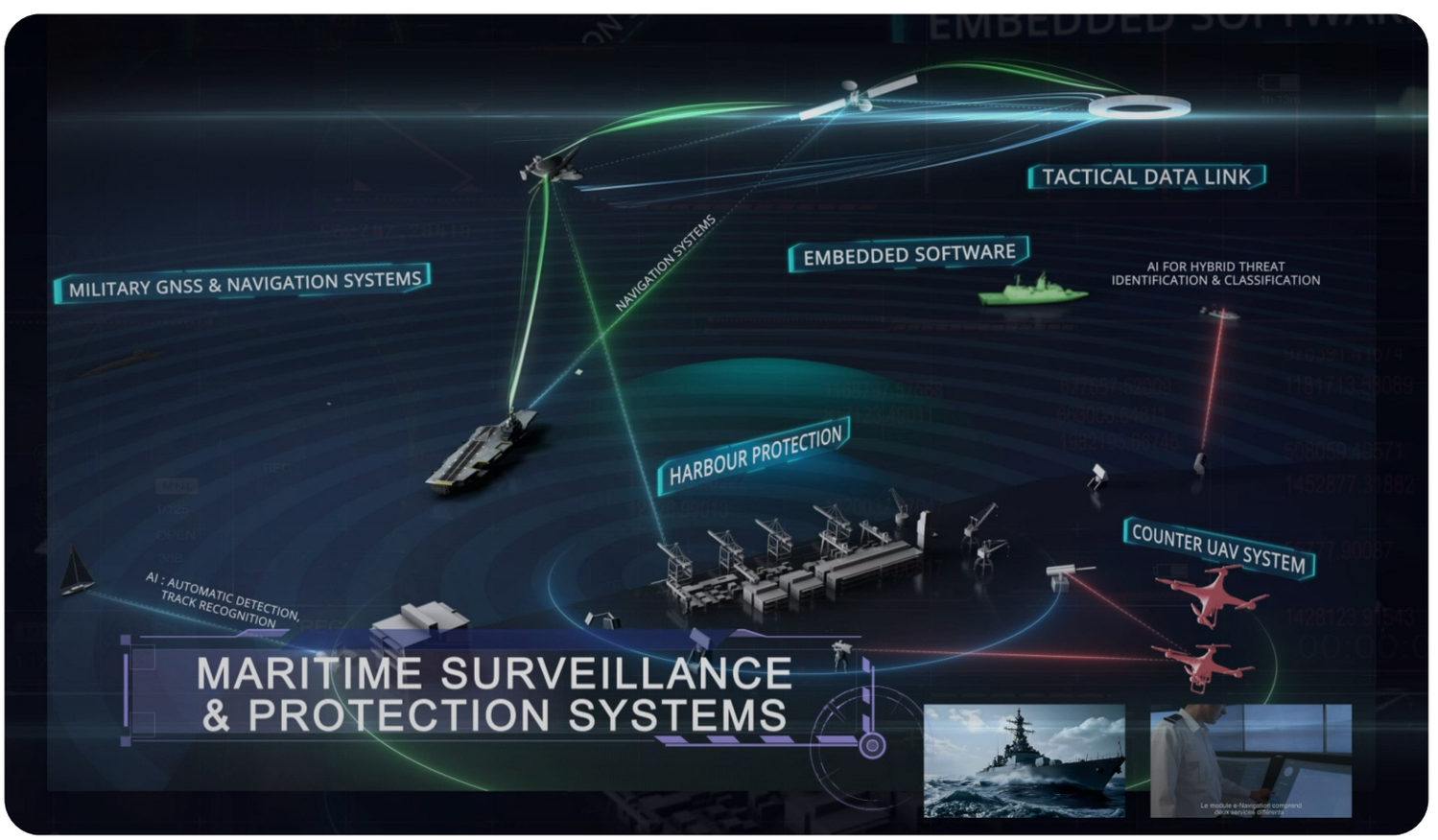
Ces 2 solutions métier sont basées sur notre architecture hardware commune Cysway.

Grâce à ces solutions, CS GROUP offre aux navires des capacités accrues en matière de navigation sécurisée, de protection contre les interférences et de coordination tactique, renforçant ainsi leur efficacité opérationnelle.

Fort de plus de 150 systèmes installés à bord, pour les marines française, étrangères ou de l'OTAN, CS GROUP s'impose ainsi comme un acteur clé dans le développement de solutions technologiques avancées répondant aux besoins spécifiques de la Marine nationale, en opération ou à l'entrainement. Que ce soit à travers ses systèmes de Command & Control, ses solutions de protection portuaire ou encore ses innovations dans la lutte anti-drones et la navigation embarquée, CS GROUP offre une palette d'outils performants, alliant cybersécurité, résilience et innovation technologique.

Ces solutions, déjà éprouvées dans des contextes opérationnels, renforcent la sécurité, la précision et l'efficacité des missions militaires et navales sans oublier que la mer est en synergie avec la terre, l'air, l'espace et le cyber.

**La combinaison de nos expertises et de nos solutions se fait ainsi au profit des opérations multi-domaines. Sopra Steria et sa filiale CS GROUP se sont résolument engagés sur cette voie à la croisée de leurs domaines d'expertise et de leurs solutions.**






The world is how we shape it*